The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.9
USAP Information Security Awareness, Training and Education Program

Organizational Function	Information Resource Management	**Policy Number**	5000.9
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	**Effective Date**	1 August 2004
		Review On	1 August 2006
Subject	Awareness, Training & Education	**Authorized By**	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	**Responsible Official**	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	**Phone**	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov/od/opp
Distribution	USAP-Wide	**Status**	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

This directive establishes the Information Security Awareness, Training and Education Program for information resources supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP).

2. BACKGROUND

An Information Security organization is required to implement federal information technology regulations regarding security of information and information resources.

3. Guiding Principles

- The Information Security Awareness program will address the information security concerns that apply to USAP science and operations mission needs

4. Policy

All users of USAP information resources must receive training in information security commensurate with the responsibilities of their role within the USAP.

4.1 Operational Definitions

4.1.1 Information Security Awareness Program

An Awareness program mixes Awareness training sessions with periodic reminders and promotional materials to bring the attention of information resource users to information security issues, and to increase their understanding of vulnerabilities and threats affecting the security of USAP information. An Awareness program is typically geared towards the non-technical user community, or technical users outside an organization's Information Technology group. The Federal Information Security Management Act of 2002 (FISMA) and OMB Circular A-130 require all users of federal information resources to receive periodic Awareness training as part of an Awareness program.

4.1.2 Information Security Training

Information Security training is typically considered technical training, and it focuses on improving the security skills and competencies of personnel managing, designing, developing, acquiring, and administering information resources. Technical training is intended for information security staff, and for information technology staff in positions with security related responsibilities, such as system administrators or network engineers. Technical training typically includes short courses, seminars, professional development workshops, conferences, and certificate programs. Technical training is provided to staff by the parent organization, to ensure the staff member is able to accomplish their duties.

4.1.3 Information Security Education

Information Security education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles, and strives to produce information security specialists and professionals capable of vision and pro-active response. Typically, education involves a long-term course of study at the university level, and is provided to staff at the discretion of the parent organization.

4.2 The USAP Information Security Awareness, Training and Education Program.

The USAP Information Security Manager (ISM) shall establish a program to provide Awareness, Training, and Education for all users of USAP information resources, commensurate with the responsibilities of their duties within the USAP. This program will categorize users according to their position responsibilities, identify training goals, and prepare training materials to cover subjects relevant to the secure operation of USAP information resources.

4.2.1   User Training Categories.

To provide training relevant to their needs, the user community shall be divided into the following categories:

- Senior management responsible for setting USAP policy.

- Mid-level managers and supervisors with program or functional responsibility for the security of USAP information resources.

- Technical staff responsible for daily operations of USAP information resources or the development and implementation of information systems or applications.

- End users of USAP information resources who rely on these resources to accomplish their specific duties within the USAP.
- Science team members who use USAP information resources incidentally in the course of completing their research grant activities.

4.2.2   Training Subject Matter.

The ISM will incorporate the following subjects into the development of training materials, as appropriate for each audience.

- Basic Concepts of information security practices, and the importance of protecting information from known vulnerabilities or threats, to include the reporting of security weaknesses and vulnerabilities. Includes an orientation to specific information security concerns of the USAP operations environment and an explanation of the user's interface with the USAP information security program.

- Security Planning and Management, which includes risk analysis and management, intrusion prevention and penetration testing, the determination of security requirements, security training, and the internal organization responsible for information security

- Information Security policies, processes, standards and procedures for all areas of information security relevant to the audience

- Contingency Planning, to include preparations, backup plans, disaster recovery, and continuity of operations

- System Lifecycle Management, which explains how information security is addressed during each phase of the system life cycle, including procurement, certification, and accreditation of information systems
- Advanced Security Topics, which covers skills needed to install preventive security controls, analyze log data for intrusion detection, assess risks and vulnerabilities, establish system rules, conduct self-evaluations, evaluate the impacts resulting from implementing security controls, plan risk reduction activities, and conduct testing of contingency plans. Technical training courses may be suitable substitutes for training in these topics.

4.2.3   Training Levels and Goals.

The level of training in each subject area will vary across the USAP from general awareness to specific courses depending on each user's job responsibilities. The levels of training are as follows:

- **Awareness training.** This level of training is expected to increase the user's sensitivity to threats and vulnerabilities, and the need to protect information. It includes information on the USAP context for information security, and on USAP instructions and processes that directly affect the user community

- **Policy Training.** This level of training improves understanding of information security principles so that informed policy decisions about information security programs can be made

- **Implementation Training.** This training will provide users the ability to recognize and assess the threats and vulnerabilities to information resources, so that security requirements can be set to fulfill USAP policies, and procedures

- **Performance Training.** Performance training will provide users the skills necessary to design, execute, and evaluate USAP information security policies and procedures. The recipient of this training shall be able to apply security concepts while performing their job responsibilities, typically within the IT organization.

4.3   User Participation.

All users of USAP information resources, including all members of a science grant research team, must complete USAP Information Security Awareness Training as a condition of continued use of USAP information resources. An equivalent awareness training course conducted by another federal agency may be accepted as a substitute for the USAP awareness training, provided the user is made aware of USAP-specific concerns and issues through other means. User participation in more focused technical training and education activities is based upon position duties and requires management support from within the user's sponsoring organization.

4.4   Annual Awareness Training.

The ISM will establish a program to ensure all users receive Awareness training on an annual basis. Awareness training may be provided through any appropriate means, including classroom training, computer-based training, or self-study materials. Awareness training will explain user responsibilities to protect the confidentiality, integrity, and availability of information, identify current threats and vulnerabilities that may affect the security of a user's information resources, and review policies, processes, standards, procedures, or technologies that apply to the use of USAP information resources.

4.5   Record of Training.

All USAP participant organizations shall record the completion of Annual Awareness Training, and other Technical Training by their staff. By 30 June of each fiscal year, each USAP participant organization will verify to the USAP ISM that their users of USAP information resources have completed the USAP or other appropriate federal information security awareness training program. The principal investigator of each science team shall forward written notice verifying their affected team members have completed the USAP or other federal awareness training program, prior to commencing their science activities for the season.

4.6   Awareness Training Opportunities.

The ISM will schedule multiple opportunities throughout the year for USAP users to complete their Awareness Training requirements. When possible, awareness training will be conducted in conjunction with other USAP training, or other USAP events that include large participant groups. Examples include the annual science user committee meetings, pre- and post-deployment orientation, and web-based training materials.

4.7   Funding.

Each participant organization is responsible for funding information security technical training and education for their staff.

5.   APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program.*

6.   RESPONSIBILITIES

6.1   NSF Technology Development Manager.

The NSF Technology Manager oversees the development and implementation of the Awareness, Training and Education program as part of the overall USAP information security program.

6.2   USAP Information Security Manager (ISM).

The ISM develops and implements the InfoSec AT&E program and coordinates its activities with the NSF Information Security Officer, and with other USAP participant organizations. The ISM ensures that Information Security Awareness, Training, and Education activities are included in project plans and budgets as appropriate.

6.3 USAP Participant Organizations

The USAP participant organizations, to include the various science teams, support the USAP ISM with the development and implementation of the Awareness program. This support includes ensuring that all affected members of their organization complete the appropriate level of training required for participation in the USAP.

7. PROGRAM IMPLEMENTATION

7.1 Program Administration.

The ISM will establish an Information Security Awareness, Training and Education program to include all users of the USAP information resources. Program objectives will be included in the annual Information Security plan.

7.2 Processes, Standards and Procedures

The ISM will establish processes, identify standards, and develop procedures to support the Awareness, Training and Education program.

7.3 Awareness Training

The ISM will ensure awareness training opportunities are made available to all USAP users.

7.4 Technical Training and Education

The ISM will identify suitable technical training and education programs to support USAP technical staff.

7.5 Record of Training Completion

The ISM will track the completion of Awareness training by users of USAP information resources, and report training statistics to OPP annually.

7.6 Policy Review.

The USAP Information Security Program Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director